Copy to D.D(C&A)
13/8

15 (I)

TOP SECRET"U" 1 TICOM/I-64

ANSWERS BY WM. BUGGISCH OF OKH/CHI

to QUESTIONS SENT BY TICOM.

Attached are a) questions sent by Ticom to be put to Wm. OTTO BUGGISCH of OKH/HNW/Gen d. NA, held at 6824 DIC.OBERURSEL, and b) BUGGISCH'S answers, supplied in interrogation to Major W.P. Bundy,AUS.

TICOM
8Aug.1945

Copy No. 12
No of pages 4

Distribution

British
1. Director
2. D.D.3
3. D.D.4
4. D.D.(N.S.)
5. D.D.(M.W.)
6. D.D.(A.S.)
7-8A.D.(C.C.R)(2)
9. Lt. Col. Leathem

U.S.
26-27 OP 20-G(2)(via Lt. Pendergrass)
28 G-2(via Lt. Col. Hilles)
29-30 S.S(A.(2)(via Major Seaman)
31. Director, S.I.D. USFET
(via Lt. Col, Johnson)

TICOM
10. Chairman
11-12 S.A.C.(2)
13. Cdr. Bacon
14. Cdr. MacKenzie
15. Cdr. Tandy
16. Lt. Col. Johnson
17. Lt. Col. Lewis Powell
18. Lt. Cdr. Manson
19. Major Seaman
20. Lt. Eachus
21. Lt. Vance
22. Capt. Cowan
23. Lt. Fehl
24-25 Ticom Files(2)

Additional
32 Major G.W.Morgan
33 Lt. Col. Pritchard
34 Mr Twinn

A. On July 27, 1945. Ticom requested that the following question be put to Buggisch:

1. Describe in detail the Russian systems on which you worked, and the breaking methods used.

2. Can you state how many M-209 keys were broken monthly at OKW/Chi or elsewhere?Give units and personalities, if recalled, which appeared in the decodes.

3. What was the extent of liaison with the Japanese at various units with which you worked? On what systems did liaison exist?

4. Describe more fully the organisation and work of WAPRUEF 7, including strength.

5. Can you give further details of the K37?

6. What success did they have on Swedish Hagelin?

B. The following replies have been obtained from Buggisch.

1.Russian Systems

In 1943 B heard that the Forschungsamt (no individual names given) had claimed some success on a Russian teletype machine, and had re-created the action of the machine. It was a machine with a very long cycle being not prime but the product of several smaller cycles--like the SZ42. B. did not know the cycle of all of the individual wheels or any other details. He heard this from DOERING,who was then doing his research on the T52, but liaison with the FA was bad anyway(Major Mettig was particularly opposed to the SS taint) and the next he heard was that the traffic found by the FA had stopped. B. remembered only that the cycle of one wheel was 37; the others, he thought, varied widely from 30-80.

Late in 1943 and increasingly in 1944 OKH itself began to intercept non-Morse,5-impulse traffic(called "Hughes" by B.) The Mathematics Referat went to work on it ,with TROEBLICHER playing a leading part. At the end of 1943 the Russians created a "kompromiss", giving a depth of about 8 messages with the same setting. With this they were able to recover 1400 letters of pure key and at the same time to ascertain that the traffic being passed was the 5-figure code, withregular station chat enciphered at the same time on the machine(Suggests a machine in constant motion as described by Karrenberg).Part of the depth was created within the same long message, so that the machine had a cycle, at least in this one case of about 1450 letters. The actual number was thought to be very significant by the Germans, as it was prime and so could not be the product of smaller cycles in any way that they could imagine. This differentiated it from the machine which the FA had broken. The Germans postulated either a single tape machine like the T43 or a machine in which the motions of the wheels influenced each other,1 and 2 affecting 3, 3 affecting 5, etc. as in the T52. They were never able to prove one theory or the other. (B. apologised for this.Said they did not have enough mathematicians to tackle the fascinating problem of determining what the motion must be to create this cycle. Seemed quite convinced that there would be a unique solution to the problem.).....After this experience they devised Hollerith machinery to locate depths, but in fact they only found three or four more cases and none of thes gave additional cycle evidence or even furnished as much pure key as the first one. B. left the section in June 1944. He thinks the traffic slumped off in the summer of 1944, and LNA took steps to try to improve the reception, as they believed the traffic was still there. TROEBLICHER was detailed to this end of the work at this time.

B. stressed one fact which had surprised him, that they had never had information about either of these machines(he assumed that the one the FA

broke was not the same because of the difference on cycles.) from PW or agent sources.

B. said in passing that their own security idea on the subject of wheel machines of this sort was that the cycle should not be the product of smaller periods(as in Hagelin) even if this was long. Mutual influence of wheels should be used to avoid this, but at the same time care must be taken that too short a period was not created in the process. This in fact had apparently been done by the Russians, but the fact that it was not repeated suggested to him that they might have seen the weakness and corrected it.

On other Russian systems B. was unable to add much to what he had stated before. His own immediate work had been in the field only in 1941. He knew that the breaking had been so important in 1942 that the best man on it, PIETSCH, had been sent to Heeresgruppe Sued to be in on the operational breaking there. At this time they had only had depths of 2 but were still able to solve almost all the traffic on the use of place names and set phrases giving very common code groups. This success continued up the fall of 1942, after which time the use of Blocknote became increasingly prevalent, and breaking slumped accordingly.

B. also had heard from von DENFFER that the latter had had great success in the Northern front on NKWD in the winter of 1942-3. No details known.

B. mentioned the following personalities in the Russian field. Uffz. RADEMACHER, Wm. SAMSANOV. KRAUT. These men were all Russian speakers(the best of the "KAUFLEUTE" of whom B. speaks in general with disgust.)

2.M209

B. stated that the operational breaking of 209 was done by the KDRE and he was quite unable to give details. Neither OKW nor OKH worked on it operationally as far as he knew.

3. Liaison with the Japanese

Use of the "Verbindung" led B. promptly into a long discussion of Jap systems in particular and diplomatic systems in general, but when we finally pinned him down to crypt relations he said he did not know about OKW--but had never heard of any-- and as for OKH he was sure that there had never been any Japs around in the flesh or any liaison he knew of.

The previous discussion of systems got onto some interesting ground. B. thinks Steinberg(of 209 fame) solved some Jap machine traffic which was difficult but not so hard as Enigma.B. thinks it was traffic of the Jap Military Attache. HUETTENHAIN told B. that the Japs were using Enigma in their traffic to TOKYO--or so B. remembers. Later he said Enigma was used almost 100% on all diplomatic links at the end of the war, and we checked him back and asked if he did not mean that the Germans used Enigma to TOKYO, not the Japs. He said he thought it was both, again from hearsay. HUETTENHAIN had also told B that the diplomatic traffic was Enigma with some element of the key,Stecker he thought, changed from message to message.

B. also spoke of the use of a "G" machine, like the Enigma, but with no stecker, and with several notches on the wheels, This was used by the Abwehr and also by Military Attaches. HUETTENHAIN had thought it not so secure as the Military Enigma, and eventually it had been replaced by the latter.

4. Wapruef 7

B. stressed that LIEBKNECHT had been with this outfit far longer than he and would really know the score on it. His own picture, however, does credit to his memory for names and section names.

There were seven Gruppen.

Gruppe I--Verwaltungssachen---relations with industry in general. Headed by a Min Rat whose name he could not recall.

Gruppe II--Drahtverbindung--headed by Major Dressler

Gruppe III--Development of cipher devices, scramblers, and all matters of this sort. Headed by Oberstlt PAECHTER. Liebknecht, the only one B. knew in this, could not estimate its total strength.(L. gives a picture of a very small outfit, with only two or three men on each job, so that L. was never able to do original work and in fact had to spend a large share of his time simply visiting labs.) This Gruppe was split up at the end and part moved to Planken which was 30 km from Staats, where B. was, so that there was more contact, but not closely so.

Gruppe IV-- Development of counter measures to enemy security devices as in III.Headed by Oberstlt WEIDEMANN, with Major Zschocker as his deputy. Major Z. was head of Ref A, which had to so with building problems. Ditto Ref. B. Ref. C was the Baudot section, headed by OberBau Rat Keirkhoff. Sonderfueher BRITSCHNEIDER also prominent in section. There were about 5-6 engineers, 7-8 other men, and 60 odd Nachrichtenhelferinnen in the section.The bulk of the work was on Russian Baudot. American traffic could be intercepted.(B. got off onto this, said it was never broken at OKH.Ten letter indicators were used, and he remembered no further details.They had too few men to do the job.).....Ref. D. had to do with Peilgeraeten, with DF maps and reports, and also with photographic work.(Just how these two mingled was not clear either to B. or to interrogators.)...And Ref E was B's own section on speech scrambling with 8 people under Dr. Lotze.(From the tenor of his references we inferred that this was a typical size for a referat on one field. The KEIRKHOFF referat was definitely outsize in the organization.)

Gruppe V--Festungsfunk problems. No details known.

Gruppe VI--had been abolished,B. believes.

GruppeVII--Fernsteuerung. Headed by a Min Rat whose name could not be recalled. 15 or so of this group came out to Staats at the end of the war, but B. did not know what the total strength of the outfit had been.

5. K37

This was an electrical machine, almost exactly similar to the French B 211 but without the "Ueberschluesseler"(added E. wheel at one point) of the B211. It was considerably less secure than the B211 and a theoretical solution was worked out which did not need much text. B. had forgotten the details on this. The K37 had been captured, but never really used by the Russians.

6.Swedish Hagelin

B.'s only knowledge came from a talk with HUETTENHAIN. H. told him that in the summer of 1943 a civilian mathematician in OKW. had solved a 5000 letter message on the Swedish machine by statistical methods. This was the only solution of which he had ever heard.His recollection was that the solved key contained no overlaps.(The task of explaining overlap to the dumb-playing interrogators was almost too much for him until he thought of 209.)